Elliptic curve IV

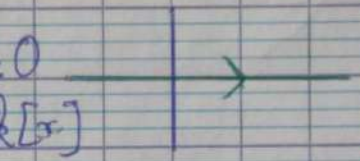
Part 2: Pairings:

Goal: define the Weil and Tate pairings on an elliptic curve $E/\mathbb{F}_q$

Today: functions on E and poles and zeroes, multiplicities

I) Function field of a curve:

Definition: Let $\mathcal{C}: f(x,y)=0$ be a plane curve/k. The function ring of $\mathcal{C}$ is $k[\mathcal{C}] := k[x,y]/f(x,y)$



example: $\mathbb{A}^1$ is given by $y=0$
$k[\mathbb{A}^1] = k[x,y]/(y=0) \simeq k[x]$

example: $E: y^2 = x^3 + ax + b$, $k[E] := k[x,y]/(y^2 - x^3 - ax + b)$

Warning: $k[\mathcal{C}]$ depends on the affine model of $\mathcal{C}$

Definition: Let $\bar{\mathcal{C}}$ be a smooth integral projective curve, and $\mathcal{C}$ be any affine model.
Then $k(\bar{\mathcal{C}}) = k(\mathcal{C}) := \mathrm{Frac}\, k[\mathcal{C}]$ does not depend on the model $\mathcal{C}$.

Example: $k(\mathbb{P}^1) = k(\mathbb{A}^1) = \mathrm{Frac}\, k[x] = k(x)$

$E: y^2 = x^3 + ax + b$, E is irreducible so $k[E]$ is integral
$k(E) = k(x)[y]/(y^2 - x^3 - ax - b)$

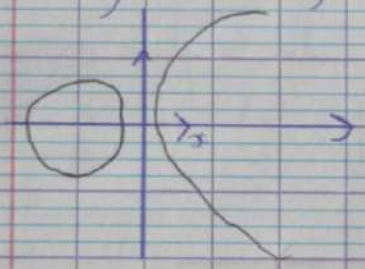
Theorem: "The function field of $\mathcal{C}$ is ~~smooth~~ enough to recover $\mathcal{C}$"
If $k = \bar{k}$ is alg closed, there is an equivalence of categories between smooth integral projective curves and fractional morphisms of curves, and function fields of transcendence degree 1 over k and morphisms of field

Remark: If E/k is an elliptic curve, $k(E)$ is a quadratic extension of $k(\mathbb{P}^1) = k(x)$
Geometrically, this corresponds to the morphism (of degree 2)

$E \longrightarrow \mathbb{P}^1$

$(x,y) \longrightarrow x$

$(X:Y:Z) \longrightarrow (X:Z)$



Examples of rational functions on E:

$$r(x,y) = \frac{a_1(x) + a_2(x)\,y}{b_1(x) + b_2(x)\,y}$$

If $r(x,y) = a_1(x) + a_2(x)\,y$ then $\bar{r}(x,y) = a_1(x) - a_2(x)\,y$

$N(r) = r\bar{r} = a_1^2 - y^2 a_2^2 = a_1^2 - (x^3 + ax + b)\,a_2^2 \in k(x)$

$r' = \frac{r_1}{r_2} = \frac{r_1 \bar{r}_2}{r_2 \bar{r}_2} = \frac{r_1 \bar{r}_2}{N(r_2)} \in k(x)$

$r(x,y) = c_1(x) + y\,c_2(x)$ with $c_1, c_2 \in k(x)$

$x - x_P$ will have a zero at P — $\frac{1}{x - x_P}$ will have a pole at P

$\frac{y - y_P}{x - x_P}$ what's the value at P?

II) Poles, zeroes and multiplicities:

1) Uniformizers on curves

Let $\mathcal{C}$ be a smooth curve and P be a point.
Define $k[\mathcal{C}]_P = \{r \in k(\mathcal{C})$ such that r does not have a pole at $P\}$
$m_P \subset k[\mathcal{C}]_P = \{r \in k(\mathcal{C}) \mid r$ has a zero at $P\}$

Theorem: $k[\mathcal{C}]_P$ is a discrete valuation ring and m_P its unique maximal ideal.

Corollary: m_P is principal.
$m_P = (\Pi_P)$, Π_P a uniformizer at P, and if $r \in k(\mathcal{C})$, $r = u\Pi_P^n$, u has no zero or poles at P, i.e. u is invertible in $k[\mathcal{C}]_P$, and $n \in \mathbb{Z}$ is the multiplicity of r at P.
- If $n > 0$, r has a zero at P of mult n
- If $n < 0$, r has a pole at P of mult n
- If $n = 0$, r has no pole or zero at P

Definition: $v_P(r) = n$ is a discrete valuation
Recall that this means: $v_P(r_1 r_2) = v_P(r_1) + v_P(r_2)$
$v_P(r_1 + r_2) \geq \min(v_P(r_1), v_P(r_2))$

Remark: Π_P is a uniformizer at $P \iff$ every r can be written as $r = u\Pi_P^n \iff$ $v_P(\Pi_P) = 1$.

Proposition: Assume that $k = \bar{k}$ $\mathcal{C}$ projective
1) If $P \in \mathcal{C}$, v_P is a valuation on $k(\mathcal{C})$
2) Conversely, any valuation v on $k(\mathcal{C})$ corresponds to a point $P \in \mathcal{C}(\bar{k})$

2) The projective line:

$k(\mathbb{P}^1) = k(x)$

$P: \; x = a$

If $r(x)$ is a polynomial in x and $r(a) = 0$, we can write $r(x) = (x-a) r_1(x)$

$\Rightarrow$ if $r(x) \in k(x)$, $r(x) = (x-a)^n r_1(x)$ with r_1 having no pole or zero at $x = a$.

$\Rightarrow x - a$ is a uniformizer

$v_{x=a}(x-a) = 1$

Example: if $P: \; x = 0 \Rightarrow$

$-v_P(x^3) = 3$: zero of multiplicity 3

$-v_P\left(\frac{x^2+x}{x^4}\right) = -3$ pole of mult 3.

$\Rightarrow$

$v_P(x^2+x) = v_P(x^4) = \min(2, 1) - 4 = 1 - 4 = -3$

Example: $-\deg$ is a valuation on $k(x)$

$\deg(P_1 P_2) = \deg(P_1) + \deg(P_2)$

$\deg(P_1 + P_2) \leq \max(\deg(P_1), \deg(P_2))$

This corresponds to the point at infinity.

Prop: $P = \infty$ corresponds to $y = 0$ under the change of variable $y = \frac{1}{x}$

$v_{x=\infty}(x^n) = v_{y=0}\left(\frac{1}{y^n}\right) = -n = -\deg(x^n)$

example: $r = \frac{x^3 + x + 1}{x^2 + 3x} = \frac{X^3 + XZ^2 + Z^3}{X^2 Z + 3XZ^2}$

$\deg(r) = \deg(x^3 + x + 1) - \deg(x^2 + 3x) = 3 - 2 = 1$

$v_\infty(r) = -1$

So r has a pole of mult 1 at $P = \infty$

Aside: Every function $r \in k(\mathcal{C})$ defines a morphism $r: \mathcal{C} \to \mathbb{P}^1$
We say that $r(P)$ is the value of r at P.
- $r(P) = 0$ if $v_P(r) > 0$
- $r(P) = \infty$ if $v_P(r) < 0$
- If $v_P(r) = 0$, $r(P) = a$, $a \neq 0$, $a \neq \infty$

$r = \frac{r}{x_2} x_2 = \pi_P^n u = u$ $\quad r = 0$ if $v_P(r) = 0$

example: $P: x = 1$

$r = \frac{x^2 - 1}{x - 1} = \frac{(x-1)(x+1)}{x-1} = x + 1$ so $r(1) = 2$

3) Elliptic curve:

* $P = (x_P, y_P)$, with $y_P \neq 0$, P is not a ramification point

Theorem: $\pi_P = x - x_P$ is a uniformizer

Lemma: $v_P(r) = v_{-P}(\bar{r})$

Proof: $r = a(x) + b(x)y$ with $a, b \in k[x]$
Assume that $r(P) = 0$
- if $r(-P) = 0$

$\begin{cases} a(x_P) + b(x_P) y_P = 0 \\ a(x_P) - b(x_P) y_P = 0 \end{cases} \Rightarrow \begin{cases} a(x_P) = 0 \\ b(x_P) = 0 \end{cases}$

$r = (x - x_P) r_1$

Iterating: $r = (x - x_P)^n r_2$ where either $r_2(P) \neq 0$ or $r_2(P) = 0$, $r_2(-P) \neq 0$

$r_2 = \frac{r_2}{\bar{r}_2}$ $\quad \frac{1}{r_2}(P) = r_2(-P) \neq 0$

$r_2 = \frac{N(r_2)}{r_2} \in k(x)$ $\quad r_2 = \frac{(x - x_P)^m r_3}{\pi_2}$ and $\frac{r_3(P)}{\pi_2(P)} \neq 0, \infty$ and $\frac{r_3}{\pi_2}(P) \neq 0, \infty$

$r = u(x - x_P)^{n+m}$ with $u(P) \neq 0, \infty$

summary: $v_P(x-x_P)=1$, write $r=(x-x_P)^n r_1$ with $v_P(r_1)=v_P(\bar{r}_1)=0$

So $v_P(Nr_1)=v_P(r_1)+v_P(\bar{r}_1)=v_P(r_1)$

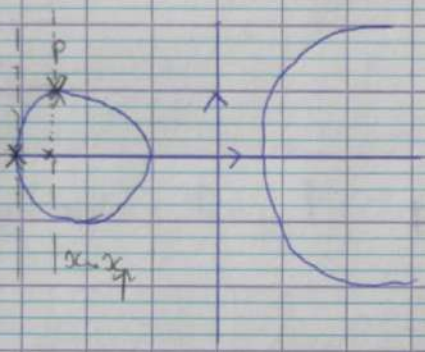
So $v_P(r_1)=v_P(Nr_1)=v_{x=x_P}(Nr_1)$

and $v_P(r)=n+v_P(r_1)=n+v_{x=x_P}(Nr_1)$

*P a Weierstrass point, $P=(x_P,0)$

Theorem: $\Pi_P=y$ is a uniformizer

$v_P(x-x_P)=2$



$$x-x_P=\frac{y^2}{(x-x_Q)(x-x_R)}$$

Proof: "Don't write it entirely but get the summary"

Summary: If $r=a(x)+yb(x)$

$v_P(r)=\min(2v_{x=x_P}(a(x)),\ 1+2v_{x=x_P}(b(x)))$

$v_P(r)=v_{-P}(\bar{r})=v_P(\bar{r})$ because $P=-P$

$v_P(N(r))=2v_P(r) \Rightarrow v_P(r)=v_{x=x_P}(Nr)$

$N(r)$ since $v_P(x-x_P)=2$

*$P=O_E$ the point at infinity

Theorem: $v_{O_E}=-\deg$

Δ $y^2=x^3+ax+b$: $2\deg(y)=3\deg(x)$

$\deg(x)=2$

$\deg(y)=3$

Corollary: $\Pi_{O_E} = \frac{x}{y}$ is a uniformiser

Proof: $\deg\left(\frac{x}{y}\right) = \deg(x) - \deg(y) = 2 - 3 = -1$

Example: x and y both have a pole at O_E of mult 2 respectively 3.
If $\Lambda = \frac{xy}{x}$, $\Lambda(O_E) = \infty$ because $v_{O_E}(x) = -\deg(x) = -1$